

REMARKS

The Office Action of July 12, 2004 was received and carefully reviewed. By this Amendment, claims 1, 15, and 20 are amended, claims 16-17 are canceled, and new claims 21-29 are added. Support for these amendments can be found throughout the specification, specifically, on pages 24 to 28. In light of the above amendments and for the reasons advanced in detail below, reconsideration and withdrawal of the currently pending rejections is respectfully requested.

As is shown on pages 2-5 of the Office Action, claims 1, 4-7, 12-17 and 19-20 stand rejected under 35 U.S.C. 102(e) as being anticipated by Wiser et al. (U.S. 6,385,596). Thus, the Examiner asserts that Wiser et al. teach each and every element of independent claims 1 and 15, and dependent claims 4-7, 12-14, 16-17, and 19-20. This rejection is respectfully overcome, as Wiser et al. fails to disclose all of the features recite in independent claims 1 and 15, as amended, and as set forth below.

Amended independent claim 1 recites a method for encrypting an original message to be passed to a recipient by way of a grantor, the method comprising the steps of obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor according to a public key encryption scheme, generating a public proxy key based on a private key corresponding to the recipient and on the private key corresponding to said grantor, wherein said grantor's private key and said recipient's private key are combined, and the combination of the private keys is based on said public key encryption scheme and provides that it is computationally difficult to recover the recipient's private key from the public proxy key even with the knowledge of the grantor's private key, and applying the public proxy key to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and the available public key information.

Independent 15 recites a method for encrypting an original message to be passed to a recipient by way of a grantor, the method comprising the steps of obtaining an encrypted

message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor according to a public key encryption scheme, generating a public proxy key based on a public key corresponding to the recipient and on the private key corresponding to the public key of said grantor, wherein said grantor's private key and said recipient's public key are combined, and the combination of said grantor's private key and said recipient's public key is based on said public key encryption scheme, and applying the public proxy key to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient's public key and the available public key information.

Wiser et al. disclose a secure online music distribution system wherein a media key used of encryption is itself encrypted. An audio image is encrypted with a symmetric media key, which is preferably a strong random number. (Col. 7, lines 27-29). The media key is separately encrypted with a public key of a content manager. (Col. 7, lines 38-41). Upon delivery of the encrypted audio image, the content manager's public key encryption of the media key is decrypted, and the media key is re-encrypted with a public key of the user's media player (recipient). (Col. 7, lines 42-46). Thus, the media key itself is protected via encryption first by the grantor's public key and then subsequently by the recipient's media player public key. Thus, this encryption "locks the media key" and the audio image is also locked to the recipient's media player. (Col. 7, lines 44-46).

The invention recited in independent claims 1 and 15, as amended, generally includes (1) obtaining an encrypted message encrypted with a public key, (2) generating a public proxy key, and (3) applying the public proxy key to transform the encrypted message into a transformed message. To the contrary, Wiser et al. disclose encrypting a message with a single media key, which is then encrypted to prevent the encrypted original message from being decrypted without first decrypting the encrypted media key. Wiser et al. do not teach generating a public proxy key based on public and/or private keys from the grantor and recipient. Furthermore, Wiser et al. do not teach applying such a public proxy key to the already encrypted message to create a transformed message, as recited in independent claims

1 and 15, as amended.

Thus, Wiser et al. do not disclose each and every feature of the invention, as recited in independent claims 1 and 15, as amended. Similarly, Wiser et al. do not disclose each and every feature of the claims dependent on independent claims 1 and 15. Accordingly, Applicant respectfully requests that the rejection of claims 1, 4-7, 12-17 and 19-20 under 35 U.S.C. § 102(e) be immediately withdrawn.

Claims 2-3, 8-11 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al. and in view of Mittra (U.S. 5,748,736). This rejection is respectfully overcome.

As described above, Wiser et al. do not disclose generating a public proxy key based on public and/or private keys from the grantor and recipient. Furthermore, Wiser et al. do not disclose applying such a public proxy key to the already encrypted message to create a transformed message, as is recited in the amended claims. Moreover, the steps of generating and applying a public proxy key (based on either a private key corresponding to the recipient and a private key corresponding to the grantor or a public key corresponding to the recipient and on a private key corresponding to the public key of the grantor) to the encrypted message would not have been obvious to a person of ordinary skill in the art at the time of the invention based on the disclosure of Wiser et al.

Furthermore, even if the Examiner's assertions are correct that Mittra discloses decrypting an encrypted message and then re-encrypting the message along with digitally signing the message, the combination of the disclosures of Mittra and Wiser et al. still do not teach or suggest applying a public proxy key to an already encrypted message to create a transformed message, as recited in independent claims 1 and 15, as amended. Moreover, the steps of generating and applying a public proxy key (based on either a private key corresponding to the recipient and a private key corresponding to the grantor or a public key corresponding to the recipient and on a private key corresponding to the public key of the grantor)) to the encrypted message would not have been obvious to a person of ordinary skill in the art at the time of the invention based on the combined teachings of Wiser et al. and Mittra.

Thus, the combined teachings of Wiser et al. and Mitra do not render obvious the claimed invention as recited in independent claims 1 and 15, as amended, or the claims dependent therefrom. Accordingly, Applicant respectfully requests that the rejection of claims 2-3, 8-11 and 18 under 35 U.S.C. 103(a) as being unpatentable over Wiser et al. and in view of Mitra (U.S. 5,748,736) be immediately withdrawn.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if the Examiner deems that any issue remains after considering this response, the Examiner is invited to call the undersigned to expedite the prosecution and work out any such issue by telephone or via the to be scheduled personal interview.

Respectfully submitted,


NIXON PEABODY LLP

Carlos R. Villamar
Registration No. 43,224

Date: January 12, 2005

NIXON PEABODY LLP
Suite 900, 401 9th Street, N.W.
Washington, D.C. 20004-2128
(202) 585-8000